

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

KEVIN WILLIAMS, individually and on behalf of
all others similarly situated,

Plaintiff,

v.

FARMERS NEW WORLD LIFE INSURANCE
COMPANY,

Defendant.

NO.

COMPLAINT - CLASS ACTION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Kevin Williams, individually and on behalf of all others similarly situated (“Class Members”), brings this action against Defendant Farmers New World Life Insurance Company (“Defendant”), alleging as follows based upon personal knowledge, information and belief, and investigation of counsel.

I. INTRODUCTION

1. This action arises from Defendant’s failure to properly secure and safeguard Plaintiff’s and thousands of Class Members’ sensitive personal identifying information (“PII”), which as a result, remains in the hands of those cyber-criminals who target Private Information for its value to identity thieves.

1 2. Due to Defendant’s deficient data security, an unauthorized party accessed and
2 exfiltrated Plaintiff’s and Class Members’ PII from the network systems of Defendant’s vendor,
3 where the data was stored without adequate protection or oversight by Defendant (the “Data
4 Breach”). The confidential PII compromised in the Data Breach includes Plaintiff’s and Class
5 names, date of birth, financial account number, personal address, and Social Security Numbers
6 (collectively, “Private Information”), causing widespread injuries and damages to Plaintiff and
7 Class Members (the “Data Breach”).
8

9 3. Plaintiff and Class Members are current and former agents of Defendant. As a
10 condition of employment, Plaintiff and Class Members were required to entrust their sensitive,
11 non-public Private Information to Defendant.

12 4. Defendant contracted Infosys McCamish Systems, LLC (“IMS”) to support and
13 facilitate Defendant’s operations and corporate functions, and provided IMS the Private
14 Information Defendant had collected from Plaintiff and Class Members. When the Data Breach
15 occurred, Plaintiff’s and Class Members’ Private Information was maintained on IMS’s network
16 systems.
17

18 5. Businesses that handle consumers’ Private Information like Defendant owe the
19 individuals to whom the information relates a duty to adopt reasonable measures to protect it
20 from disclosure to unauthorized third parties, and to keep it safe and confidential. This duty arises
21 under contract, statutory and common law, industry standards, representations made to Plaintiff
22 and Class Members, and because it is foreseeable that the exposure of Private Information to
23 unauthorized persons—and especially hackers with nefarious intentions—will harm the affected
24 individuals, including but not limited to the invasion of their private health and financial matters.
25

26 6. Defendant breached its duties owed to Plaintiff and Class Members by failing to

1 safeguard the Private Information that it collected and maintained, including by failing to
2 reasonably supervise its vendor's cybersecurity practices, which allowed criminal hackers to
3 access and steal at least thousands of individuals' Private Information in the Data Breach.

4 7. According to the November 15, 2024, notice sent by IMS on Defendant's behalf
5 to victims of the Data Breach ("Notice Letter"), on or about November 2, 2023, IMS "became
6 aware that certain IMS systems were encrypted by ransomware." The ensuing investigation
7 revealed that between October 29 and November 2, 2023, "data was subject to unauthorized
8 access and acquisition," including full names and Social Security numbers of Defendant's
9 customers.
10

11 8. Upon information and belief, the mechanism of the cyberattack and potential for
12 improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to
13 Defendant, and thus, Defendant knew that failing to take reasonable steps to secure the Private
14 Information, including ensuring its vendors implemented industry-standard and legally
15 compliant security for PII, left the Private Information in a dangerous condition.
16

17 9. Defendant failed to adequately protect Plaintiff's and Class Members' Private
18 Information—and failed to even encrypt or redact this highly sensitive data, or ensure the same
19 from its vendor that received, handled, and stored it. This unencrypted, unredacted Private
20 Information was compromised due to Defendant's negligent and/or careless acts and omissions
21 and its utter failure to protect Plaintiff's and Class Members' sensitive data.
22

23 10. Defendant breached its duties and obligations by failing in one or more of the
24 following ways: (a) to ensure its vendor designed, implemented, monitored, and maintained
25 reasonable network safeguards against foreseeable threats; (b) to design, implement, and
26 maintain reasonable data retention policies; (c) to adequately train or oversee staff and service

1 providers regarding data security; (d) to comply with industry-standard data security practices;
2 (e) to warn Plaintiff and Class Members of the inadequate data security practices of Defendant's
3 vendors collecting their Private Information; (f) to encrypt or adequately encrypt the Private
4 Information, or ensure its vendor did so; (g) to ensure its vendor handling Private Information
5 had industry-standard and legally compliant data security to protect it; (h) to recognize or detect
6 that IMS's network had been compromised and accessed in a timely manner to mitigate the harm;
7 (i) to utilize, or to ensure its vendor utilized, widely available software able to detect and prevent
8 this type of attack; (j) and to otherwise secure the Private Information using reasonable and
9 effective data security procedures free of foreseeable vulnerabilities and data security incidents.

11 11. Plaintiff and Class Members have taken reasonable steps to maintain the
12 confidentiality and security of their Private Information. In providing their Private Information
13 to Defendant, Plaintiff and the Class Members reasonably expected this sophisticated business
14 entity to keep their Private Information confidential and security maintained, to use it for business
15 purposes, and to disclose it only as authorized. Defendant failed to do so, resulting in the
16 unauthorized disclosure of Plaintiff's and Class Members' Private Information in the Data
17 Breach.

19 12. Cybercriminals targeted and obtained Plaintiff's and Class Members' Private
20 Information from Defendant because of the data's value in exploiting and stealing Plaintiff's and
21 Class Members' identities. As a direct and proximate result of Defendant's inadequate data
22 security and breaches of its duties to handle Private Information with reasonable care, Plaintiff's
23 and Class Members' Private Information was accessed by cybercriminals and has now been
24 exposed to an untold number more. The present and continuing risk to Plaintiff and Class
25 Members as victims of the Data Breach will remain for their respective lifetimes.

1 13. The harm resulting from a cyberattack like this Data Breach manifests in
2 numerous ways including identity theft and financial fraud, and the exposure of a Private
3 Information in a breach ensures that the subject individual will be at a substantially increased and
4 certainly impending risk of identity theft crimes compared to the rest of the population,
5 potentially for the rest of his or her life. Mitigating that risk, to the extent even possible, requires
6 individuals to devote significant time and money to closely monitor their credit, financial
7 accounts, and email accounts, and take several additional prophylactic measures.
8

9 14. The risk of identity theft caused by this Data Breach is impending and has
10 materialized, as Plaintiff's and Class Members' Private Information was targeted, accessed, and
11 misused.

12 15. To make matters worse, although IMS confirmed the Data Breach's occurrence
13 by November 2, 2023, Defendant waited until November 15, 2024—*nearly a year* after the Data
14 Breach happened—to inform Plaintiff and Class Members that their Private Information had been
15 compromised, diminishing Plaintiff's and Class Members' ability to timely and thoroughly
16 mitigate and address harms resulting from the Data Breach.
17

18 16. As a result of the Data Breach, Plaintiff and Class Members, suffered concrete
19 injuries in fact including but not limited to (a) financial costs incurred mitigating the materialized
20 risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred
21 mitigating the materialized risk and imminent threat of identity theft; (c) actual identity theft and
22 fraud; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to
23 actual identity theft; (f) deprivation of value of their Private Information; (g) loss of privacy; (h)
24 emotional distress including anxiety and stress in with dealing with the Data Breach; and (i) the
25 continued risk to their sensitive Private Information, which remains in Defendant's possession
26

1 and control and subject to further breaches, so long as Defendant fails to undertake appropriate
2 and adequate measures to protect the customer data it collects and maintains.

3 17. To recover for these harms, Plaintiff, on behalf of himself and the Class as defined
4 herein, brings claims for negligence, breach of implied contract, violations of the Washington
5 Consumer Protection Act, and unjust enrichment to address Defendant's inadequate safeguarding
6 of Plaintiff's and Class Members' Private Information in its custody, and Defendant's failure to
7 provide timely or adequate notice to Plaintiff and Class Members that their information was
8 compromised in the Data Breach.
9

10 18. Plaintiff and Class Members seek compensatory, nominal, statutory, and punitive
11 damages, declaratory judgment, and injunctive relief requiring Defendant to (a) disclose,
12 expeditiously, the full nature of the Data Breach and the types of Private Information exposed;
13 (b) implement improved data security practices to reasonably guard against future breaches of
14 Private Information in Defendant's and its vendors' possessions; and (c) provide, at Defendant's
15 own expense, all impacted Data Breach victims with lifetime identity theft protection services.
16

17 II. THE PARTIES

18 19. At all relevant times, Plaintiff Kevin Williams has been a citizen and resident of
19 the state of California.

20 20. At all relevant times, Plaintiff was employed by Defendant. As a condition of and
21 in exchange of employment, Plaintiff was required to, and did, provide his Private Information
22 to Defendant, and through Defendant, to IMS.
23

24 21. Defendant Farmers New World Life Insurance Company is a Washington
25 corporation with its headquarters and principal place of business located at 3120 139th Ave SE
26 Suite 300 Bellevue, Washington 98005.

III. JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because the amount in controversy exceeds \$5 million, exclusive of interest and costs, and the number of Class Members exceeds 100, many of whom (namely, Plaintiff) have different citizenship from Defendant.

23. This Court has personal jurisdiction over Defendant because it is incorporated and headquartered in Washington and engaged in substantial and not isolated activity in Washington.

24. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant operates in this District and a substantial part of the events or omissions giving rise to Plaintiff's and Class Members' claims occurred in this District, including Defendant's collecting and/or failing to secure Plaintiff's and Class Members' Private Information.

IV. FACTUAL ALLEGATIONS

A. Defendant Collected and Shared Plaintiff's and Class Members' Private Information to Operate and Facilitate its Business.

25. Defendant is an insurance and benefit company offering a range of life insurance products.

26. As part of and to facilitate its business, Defendant collects and maintains the Private Information of thousands of its current and former employees and others, including Plaintiff and Class Members.

27. As a condition and in exchange of employment and other services, Plaintiff and Class Members were required to entrust their highly sensitive Private Information to Defendant.

28. Defendant derived economic benefits from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform its operations, furnish its products and services, or generate its

1 revenue.

2 29. To operate its business and facilitate IMS's contracted support services,
3 Defendant provided Plaintiff's and Class Members' Private Information to IMS.

4 30. At all relevant times, Defendant knew IMS was storing and using its networks to
5 store and transmit valuable, sensitive Private Information belonging to Plaintiff and Class
6 Members, and that as a result, IMS's systems would be attractive targets for cybercriminals.

7 31. Defendant also knew that any breach of IMS's information technology network
8 and exposure of the data stored therein would result in the increased risk of identity theft and
9 fraud for the millions of individuals whose Private Information was compromised, as well as
10 intrusion into those individuals' private and sensitive personal matters.

11 32. In exchange for receiving Plaintiff's and Class Members' Private Information,
12 Defendant promised to safeguard the sensitive, confidential data and ensure it was used only for
13 authorized and legitimate purposes, to delete such information once there was no longer a need
14 to maintain it, and to ensure the same practices from its vendors handling the Private Information,
15 including IMS.

16 33. Indeed, Defendant's Privacy Notice, published on its website, affirms and
17 warrants in part as follows:

18 **Safeguarding your information**

19 **How We Protect Your Information**

20 Our customers are our most valued assets. Protecting your privacy
21 is important to us. We restrict access to personal information to
22 those individuals, such as our employees and agents, who provide
23 you with our products and services. We require individuals with
24 access to your information to protect it and keep it confidential.
25 We maintain physical, electronic, and procedural safeguards that
26 comply with applicable regulatory standards to guard your
nonpublic personal information. We do not disclose any nonpublic

personal information about you except as described in this notice or as otherwise required or permitted by applicable law.^[1]

34. Defendant's Privacy Notice further promises that the Private Information it collects will be used "as permitted by applicable law," including a list of specific circumstances—none of which are exposure to cybercriminals in a data breach.²

35. Upon information and belief, Defendant provided the foregoing privacy notices and policies to all customers receiving insurance and/or benefit products and services from Defendant, including Plaintiff and Class Members.

B. Defendant Owed Duties to Adopt Reasonable Data Security Measures for Private Information it Collected.

36. As part of its business, Defendant collects, uses, and controls thousands (or more) of individuals' Private Information, including that of Plaintiff and Class Members.

37. Defendant had and continues to have duties to adopt reasonable measures to keep Plaintiff's and Class Members' Private Information confidential and protected from disclosure to unauthorized third parties, and to audit, monitor, and verify the integrity of its IT networks and those of their vendors and affiliates.

38. Defendant's obligations stem from the Federal Trade Commission ("FTC") Act, 15 U.S.C. § 45, common law, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and protected from unauthorized disclosure.

39. Plaintiff and Class Members value the confidentiality of their Private Information

¹ Privacy Notice, Farmers New World Life Insurance Company, Dec. 2024, available at [https://www.farmers.com/content/dam/farmers/marketing/digital/aem/pdfs/privacy-center/09-FNWL-GLBA-Notice-Final-\(Farmers-New-World-Life-Privacy-Notice\).pdf](https://www.farmers.com/content/dam/farmers/marketing/digital/aem/pdfs/privacy-center/09-FNWL-GLBA-Notice-Final-(Farmers-New-World-Life-Privacy-Notice).pdf)

² *Id.*

1 and demand security to safeguard their Private Information. To that end, Plaintiff and Class
2 Members have taken reasonable steps to maintain the confidentiality of their Private Information.

3 40. Based on the foregoing representations and warranties and to obtain insurance,
4 employment, and/or benefit products and services from Defendant, directly or indirectly, Plaintiff
5 and Class Members provided their Private Information to Defendant with the reasonable
6 expectation and on the mutual understanding that Defendant would comply with its promises and
7 obligations to keep such information confidential and protected against unauthorized access.
8

9 41. Plaintiff and Class Members relied on these promises from Defendant, and but for
10 Defendant's promises to keep Plaintiff's and Class Members' Private Information secure and
11 confidential, would not have sought services from or entrusted their Private Information to
12 Defendant. Consumers, in general, demand security for their Private Information, especially
13 when Social Security numbers and other sensitive data are involved.
14

15 42. Additionally, by obtaining, using, and benefitting from Plaintiff's and Class
16 Members' Private Information, Defendant assumed legal and equitable duties and knew or should
17 have known it was responsible for protecting that Private Information from unauthorized access
18 and disclosure.

19 43. Defendant's duty to protect Plaintiff and Class Members from the foreseeable risk
20 of injury that inadequate data protection and unauthorized exposure of their Private Information
21 would case obligated Defendant to implement reasonable practices to keep Plaintiff's and Class
22 Members' sensitive Private Information confidential and securely maintained, to use and disclose
23 it for necessary and authorized purposes only, to ensure it was deleted from its and its vendors'
24 network systems when no longer necessary for legitimate business purposes, and to ensure the
25 same data security protocols and procedures from its vendor IMS. Defendant failed to do so.
26

1 **C. Defendant Failed to Adequately Safeguard Plaintiff’s and Class Member’s**
 2 **Private Information, resulting in the Data Breach.**

3 44. On or about November 15, 2024—*nearly a year* after the Data Breach—IMS, on
 4 Defendant’s behalf, began sending Plaintiff and other Data Breach victims the Notice Letter titled
 5 “Notice of Data Breach.”

6 45. Despite its direct employer-employee relationship with Plaintiff and Class
 7 Members, Defendant did not send separate notifications to its employees impacted by the Data
 8 Breach, relying solely on IMS’s Notice Letters to alert Data Breach victims.

9 46. The Notice Letters generally inform as follows:

10 Infosys McCamish Systems, LLC (“IMS”) writes to inform you of
 11 an incident that involved some of your personal information. IMS
 12 provides administrative and back-office support technology and
 13 services for certain Farmers New Well Life Insurance Company
 14 (“FNWL”) life insurance policies and annuities. While we are
 15 unaware of any instances since the incident occurred in which the
 16 personal information involved has been fraudulently used, we are
 17 providing you with information about the incident and steps you
 18 can take to help protect your personal information, should you feel
 19 it necessary to do so.

20 **WHAT HAPPENED?** On November 2, 2023, IMS became aware
 21 that certain IMS systems were encrypted by ransomware (the
 22 “Incident”). . . . The in-depth cyber forensic investigation
 23 determined that unauthorized activity occurred between October
 24 19, 2023, and November 2, 2023. Through the investigation, it was
 25 also determined that data was subject to unauthorized access and
 26 acquisition. . . . After a comprehensive review, it was determined
 that some of your personal information was subject to
 unauthorized access/acquisition.

WHAT INFORMATION WAS INVOLVED? The
 investigation determined that the following types of your personal
 information were involved: your name, date of birth, financial
 account number, personal address, and Social Security number.

47. Omitted from the Notice Letters are crucial details like the root cause of the Data
 Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a

1 breach does not occur again. To date, these critical facts have not been explained or clarified to
2 Plaintiff and Class Members, who retain a vested interest in ensuring that their Private
3 Information is protected.

4 48. Thus, Defendant's purported disclosure amounts to no real disclosure at all, as it
5 fails to inform Plaintiff and Class Members of the Data Breach's critical facts with any degree of
6 specificity. Without these details, Plaintiff's and Class Members' ability to mitigate the harms
7 resulting from the Data Breach was and is severely diminished.
8

9 49. Defendant could have prevented this Data Breach by requiring IMS to implement
10 such reasonable safeguards as properly securing, sanitizing, and encrypting the files and servers
11 containing Plaintiff's and Class Members' Private Information, and by supervising IMS's data
12 security during the course of its contracts with Defendant to ensure such reasonable safeguards
13 were continuously maintained, but failed to do so.
14

15 50. For example, if Defendant had ensured that IMS implemented industry standard
16 logging, monitoring, and alerting systems—basic technical safeguards that any PII-collecting
17 company is expected to employ—then cybercriminals would not have been able to perpetrate
18 prolonged malicious activity in IMS's network systems without alarm bells going off, including
19 the reconnaissance necessary to identify where PII was stored, installation of malware or other
20 methods of establishing persistence and creating a path to exfiltrate data, staging data in
21 preparation for exfiltration, and then exfiltrating that data outside of IMS's system without being
22 caught.
23

24 51. Had Defendant required, by contract and oversight, that IMS implement basic
25 monitoring and detection systems, IMS would have recognized the malicious activities detailed
26 in the preceding paragraph, which then would have stopped the Data Breach or greatly reduced

1 its impact.

2 52. Defendant did not use reasonable security procedures and practices appropriate to
3 the sensitive and confidential nature of Plaintiff's and Class Members' Private Information it
4 collected and shared with vendors, including IMS, such as requiring its vendors to encrypt files
5 containing Private Information and delete Private Information from network systems when it is
6 no longer needed, which caused that Private Information's unauthorized access and exfiltration
7 in the Data Breach.

8 53. Defendant's tortious conduct and breach of contractual obligations, as detailed in
9 this Complaint, are evidenced by its failure to recognize the Data Breach or its impacts on
10 Defendant's customers until months after cybercriminals had breached IMS network and
11 accessed Plaintiff's and Class Members' Private Information stored therein—meaning Defendant
12 had no effective means in place to ensure that cyberattacks of its vendors storing Private
13 Information were detected and prevented.

14 **D. Defendant Knew of the Risk of a Cyberattack because Businesses in Possession**
15 **of Private Information are Particularly Susceptable.**

16 54. Defendant's negligence in failing to safeguard Plaintiff's and Class Members'
17 Private Information is exacerbated by the repeated warnings and alerts regarding the need to
18 protect and secure sensitive data.

19 55. Private Information of the kind accessed in the Data Breach is of great value to
20 cybercriminals as it can be used for a variety of unlawful and nefarious purposes, including
21 ransomware, fraudulent misuse, and sale on the internet black market known as the dark web.

22 56. Private Information can also be used to distinguish, identify, or trace an
23 individual's identity, such as their name, Social Security number, and financial records. This may
24 be accomplished alone, or in combination with other personal or identifying information that is
25
26

1 connected or linked to an individual, like his or her birthdate, birthplace, or mother's maiden
2 name.

3 57. Data thieves regularly target businesses in the healthcare and insurance industries
4 like Defendant due to the highly sensitive information that such entities maintain. Defendant
5 knew and understood that unprotected Private Information is highly sought after by criminals
6 who seek to illegally monetize that Private Information through unauthorized access.

7
8 58. Cyber-attacks against institutions such as Defendant and its vendor IMS are
9 targeted and frequent. According to Contrast Security's 2023 report *Cyber Bank Heists: Threats*
10 *to the financial sector*, "Over the past year, attacks have included banking trojans, ransomware,
11 account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps
12 to deliver malware in spear-phishing campaigns."³ In fact, "40% [of financial institutions] have
13 been victimized by a ransomware attack."⁴

14
15 59. In light of past high profile data breaches at industry-leading companies,
16 including, for example, Microsoft (250 million records, December 2019), Wattpad (268 million
17 records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million
18 records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service
19 (8.3 billion records, May 2020), Defendant knew or, if acting as a reasonable business handling
20 PII, should have known that the Private Information it collected, used, and shared with IMS
21 would be vulnerable to and targeted by cybercriminals.

22
23 60. According to the Identity Theft Resource Center's report covering the year 2021,

24
25 ³ Contrast Security, "Cyber Bank Heists: Threats to the financial sector," 5, available at
[https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%2020](https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%202023.pdf?hsLang=en)

26 [23.pdf?hsLang=en](https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%202023.pdf?hsLang=en) (last visited Dec. 27, 2024).

⁴ *Id.* at 15.

1 “the overall number of data compromises (1,862) is up more than 68 percent compared to 2020.
 2 The new record number of data compromises is 23 percent over the previous all-time high (1,506)
 3 set in 2017.”⁵

4 61. The increase in such attacks, and attendant risk of future attacks, was widely
 5 known to the public and to anyone in Defendant’s industry, including Defendant itself. According
 6 to IBM’s 2022 report, “[f]or 83% of companies, it’s not if a data breach will happen, but when.”⁶
 7

8 62. Indeed, Defendant’s other service provider had recently experienced a cyberattack
 9 that exposed customer PII, just months before this Data Breach. Thus, Defendant was acutely
 10 aware of the risk of a data breach and the harm that a vendor’s inadequate data security measures
 11 would cause.

12 63. Defendant’s data security obligations were particularly important given the
 13 substantial increase, preceding the date of the subject Data Breach, in cyberattacks and/or data
 14 breaches targeting entities like Defendant and its vendors that collect and store PII.
 15

16 64. In 2023, an all-time high for data compromises occurred, with 3,205 compromises
 17 affecting 353,027,892 total victims. Of the 3,205 recorded data compromises, 809 of them, or
 18 25.2% were in the medical or healthcare industry. The estimated number of organizations
 19 impacted by data compromises has increased by +2,600 percentage points since 2018, and the
 20 estimated number of victims has increased by +1400 percentage points. The 2023 compromises
 21 represent a 78 percentage point increase over the previous year and a 72 percentage point hike
 22

23
 24 ⁵ See “Identity Theft Resource Center’s 2021 Annual Data Breach Report Sets New Record for
 25 Number of Compromises,” ITRC, Jan. 24, 2022, available at
[https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-](https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/)
[report-sets-new-record-for-number-of-compromises/](https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/) (last visited Aug. 22, 2024).

26 ⁶ IBM, “Cost of a data breach 2022: A million-dollar race to detect and respond,” available at
<https://www.ibm.com/reports/data-breach> (last visited Dec. 27, 2024).

1 from the previous all-time high number of compromises (1,860) set in 2021.

2 65. As a business in possession of customers' Private Information, Defendant knew,
3 or should have known, the importance of safeguarding the Private Information entrusted to it by
4 Plaintiff and Class Members and of the foreseeable consequences if Defendant's or its vendor's
5 network systems were breached. Such consequences include the significant costs imposed on
6 Plaintiff and Class Members due to a breach. Nevertheless, Defendant failed to implement or
7 follow reasonable cybersecurity measures to protect against the Data Breach.
8

9 66. Despite the prevalence of public announcements of data breach and data security
10 compromises, Defendant failed to take appropriate steps to protect the Private Information of
11 Plaintiff and Class Members from being compromised.

12 67. Given the nature of the Data Breach, it was foreseeable that Plaintiff's and Class
13 Members' Private Information compromised therein would be targeted by hackers and
14 cybercriminals for use in variety of different injurious ways. Indeed, the cybercriminals who
15 possess Plaintiff's and Class Members' Private Information can easily obtain their tax returns or
16 open fraudulent credit card accounts in Plaintiff's and Class Members' names.
17

18 68. Defendant was, or should have been, fully aware of the unique type and the
19 significant volume of data on IMS's network server(s), amounting to at least thousands of
20 individuals' detailed Private Information, and, thus, that these individuals would be harmed by
21 the exposure of that unencrypted data.
22

23 69. Plaintiff and Class Members were the foreseeable and probable victims of
24 Defendant's inadequate security practices and procedures. Defendant knew or should have
25 known of the inherent risks in collecting, using, and sharing Private Information and the critical
26 importance of providing adequate security for that information.

1 70. The breadth of data compromised in the Data Breach makes the information
2 particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to
3 identity theft, tax fraud, medical fraud, credit and bank fraud, and the like.

4 **E. Defendant was Required, But Failed to Comply with FTC Rules and Guidance.**

5 71. The FTC has promulgated numerous guides for businesses that highlight the
6 importance of implementing reasonable data security practices. According to the FTC, the need
7 for data security should be factored into all business decision-making.
8

9 72. In 2016, the FTC updated its publication, *Protecting Personal Information: A*
10 *Guide for Business*,⁷ which establishes cyber-security guidelines for businesses like Defendant
11 and its service provider IMS. These guidelines note that businesses should protect the personal
12 customer information that they keep; properly dispose of personal information that is no longer
13 needed; encrypt information stored on computer networks; understand their network's
14 vulnerabilities; and implement policies to correct any security problems.
15

16 73. The FTC's guidelines also recommend that businesses use an intrusion detection
17 system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating
18 someone is attempting to hack the system; watch for large amounts of data being transmitted
19 from the system; and have a response plan ready in the event of a breach.⁸

20 74. The FTC further recommends that companies not maintain Private Information
21 longer than is needed for authorization of a transaction; limit access to sensitive data; require
22 complex passwords to be used on networks; use industry-tested methods for security; monitor
23

24
25 ⁷ *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM. (2016),
26 https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Dec. 27, 2024).

⁸ *Id.*

1 for suspicious activity on the network; and verify that third-party service providers have
2 implemented reasonable security measures.

3 75. The FTC has brought enforcement actions against businesses for failing to
4 adequately and reasonably protect third parties' confidential data, treating the failure to employ
5 reasonable and appropriate measures to protect against unauthorized access to confidential
6 consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders
7 resulting from these actions further clarify the measures business like Defendant must undertake
8 to meet their data security obligations.
9

10 76. Such FTC enforcement actions include actions against entities that failed to
11 safeguard PII like Defendant. *See, e.g., In the Matter of LabMD, Inc.*, 2016-2 Trade Cas. (CCH)
12 ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that
13 LabMD’s data security practices were unreasonable and constitute an unfair act or practice in
14 violation of Section 5 of the FTC Act.”).
15

16 77. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or
17 affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice
18 by businesses, such as Defendant, of failing to use reasonable measures to protect Private
19 Information. The FTC publications and orders described above also form part of the basis of
20 Defendant’s duties in this regard.
21

22 78. The FTC has also recognized that consumer data is a new and valuable form of
23 currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated
24 that “most consumers cannot begin to comprehend the types and amount of information collected
25 by businesses, or why their information may be commercially valuable. Data is currency. The
26

larger the data set, the greater potential for analysis and profit.”⁹

79. Defendant failed to properly implement basic data security practices by failing to require and ensure its vendor IMS had reasonable and appropriate safeguards for Plaintiff’s and Class Member’s Private Information, in violation of its duties under the FTC Act.

80. Defendant’s failure to require and ensure its vendor IMS employed reasonable and appropriate means to protect against unauthorized access to Plaintiff’s and Class Members’ Private Information or complied with applicable industry standards constitutes an unfair act or practice prohibited by the FTC Act.

F. Defendant Failed to Comply with Industry Standards.

81. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution’s cybersecurity standards.

82. The Center for Internet Security’s (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.

83. In addition, the NIST recommends certain practices to safeguard systems, infra,

⁹ Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), <http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf>.

1 such as the following:

- 2 a. Control who logs on to your network and uses your computers and other devices.
- 3 b. Use security software to protect data.
- 4 c. Encrypt sensitive data, at rest and in transit.
- 5 d. Conduct regular backups of data.
- 6 e. Update security software regularly, automating those updates if possible.
- 7 f. Have formal policies for safely disposing of electronic files and old devices; and
- 8 g. Train everyone who uses your computers, devices, and network about cybersecurity.

9 84. Further still, the Cybersecurity & Infrastructure Security Agency makes specific
 10 recommendations to organizations to guard against cyberattacks, including (a) reducing the
 11 likelihood of a damaging cyber intrusion by validating that “remote access to the organization’s
 12 network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing]
 13 that software is up to date, prioritizing updates that address known exploited vulnerabilities
 14 identified by CISA[,] [c]onfirm[ing] that the organization’s IT personnel have disabled all ports
 15 and protocols that are not essential for business purposes,” and other steps; (b) taking steps to
 16 quickly detect a potential intrusion, including “[e]nsur[ing] that cybersecurity/IT personnel are
 17 focused on identifying and quickly assessing any unexpected or unusual network behavior,
 18 [e]nabl[ing] logging in order to better investigate issues or events[,] and [c]onfirm[ing] that the
 19 organization's entire network is protected by antivirus/antimalware software and that signatures
 20 in these tools are updated”; (c) “[e]nsur[ing] that the organization is prepared to respond if an
 21
 22
 23
 24
 25
 26

intrusion occurs,” and; (d) other steps.¹⁰

85. Upon information and belief, Defendant failed to require, by contract or oversight, that IMS implement and maintain industry-standard cybersecurity measures, including the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security’s Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, as well as other industry standards for protecting Plaintiff’s and Class Members’ Private Information, resulting in the Data Breach.

G. Defendant Owed Plaintiff and Class Members Common Law Duties to Safeguard their Private Information.

86. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its and/or its vendors’ possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. These duties owed to Plaintiff and Class Members obligated Defendant to (a) provide reasonable data security consistent with industry standards and requirements to protect Plaintiff’s and Class Members’ Private Information in its care and its vendor’s custody from unauthorized disclosure, and (b) ensure its vendor IMS implemented and maintained such appropriate safeguards with respect to Plaintiff’s and Class Members’ Private Information.

¹⁰ Cybersecurity & Infrastructure Security Agency, “Shields Up: Guidance for Organizations,” available at <https://www.cisa.gov/shields-guidance-organizations> (last visited Dec. 27, 2024).

1 87. Defendant owed duties to Plaintiff and Class Members to create and implement
2 reasonable data security practices and procedures to protect the Private Information in its and/or
3 their vendors' possession, including adequately training employees and others who accessed
4 Private Information on how to adequately protect Private Information.

5 88. Defendant owed duties to Plaintiff and Class Members to implement processes
6 that would detect a compromise of Private Information in a timely manner.

7 89. Defendant owed duties to Plaintiff and Class Members to act upon data security
8 warnings and alerts in a timely fashion.

9 90. Defendant owed duties to Plaintiff and Class Members to disclose in a timely and
10 accurate manner when and how the Data Breach occurred.

11 91. Defendant owed duties to Plaintiff and Class Members because they were
12 foreseeable and probable victims of any inadequate data security practices.

13 92. Defendant failed to take the necessary precautions to safeguard and protect
14 Plaintiff's and Class Members' Private Information from unauthorized disclosure. Defendant's
15 actions and omissions represent a flagrant disregard of Plaintiff's and Class Members' rights.

16 **H. Plaintiff and Class Members Suffered Common Injuries and Damages due to**
17 **Defendant's Conduct.**

18 93. Defendant's failure to implement or maintain adequate data security measures for
19 Plaintiff's and Class Members' Private Information directly and proximately caused injuries to
20 Plaintiff and Class Members by the resulting disclosure of their Private Information in the Data
21 Breach.

22 94. The ramifications of Defendant's failures to keep secure the Private Information
23 of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen
24 fraudulent use of that information and damage to victims may continue for years.

1 95. Plaintiff and Class Members are also at a continued risk because their Private
 2 Information remains in Defendant's care, which has already been shown insufficient to protect
 3 customer information and leaves such data subject to further attack so long as Defendant fails to
 4 undertake the necessary and appropriate security and training measures to protect its customers'
 5 Private Information.

6 96. As a result of Defendant's ineffective and inadequate data security practices, the
 7 consequential Data Breach, and the foreseeable outcome of Plaintiff's and Class Members'
 8 Private Information ending up in criminals' possession, all Plaintiff and Class Members have
 9 suffered and will continue to suffer the following actual injuries and damages, without limitation:
 10 (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent
 11 threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the
 12 materialized risk and imminent threat of identity theft; (d) financial costs incurred due to actual
 13 identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their
 14 Private Information; (g) loss of the benefit of their bargain with Defendant; (h) emotional distress
 15 including anxiety and stress in dealing with the Data Breach's aftermath; and (i) the continued
 16 risk to their sensitive Private Information, which remains in Defendant's possession and control
 17 and is subject to further unauthorized disclosures so long as Defendant fails to undertake
 18 appropriate and adequate measures to protect the Private Information it collects, uses, and shares.
 19
 20
 21

Present and Ongoing Risk of Identity Theft

22 97. Plaintiff and Class Members are at a heightened risk of identity theft for years to
 23 come because of the Data Breach.
 24

25 98. The FTC defines identity theft as "a fraud committed or attempted using the
 26

1 identifying information of another person without authority.”¹¹ The FTC describes “identifying
 2 information” as “any name or number that may be used, alone or in conjunction with any other
 3 information, to identify a specific person,” including “[n]ame, Social Security number, date of
 4 birth, official State or government issued driver’s license or identification number, alien
 5 registration number, government passport number, employer or taxpayer identification
 6 number.”¹²

7
 8 99. The link between a data breach and the risk of identity theft is simple and well
 9 established. Criminals acquire and steal Private Information to monetize the information.
 10 Criminals monetize the data by selling the stolen information on the internet black market to
 11 other criminals who then utilize the information to commit a variety of identity theft related
 12 crimes discussed below.

13 100. The dark web is an unindexed layer of the internet that requires special software
 14 or authentication to access.¹³ Criminals in particular favor the dark web as it offers a degree of
 15 anonymity to visitors and website publishers. Unlike the traditional or “surface” web, dark web
 16 users need to know the web address of the website they wish to visit in advance. For example,
 17 on the surface web, the CIA’s web address is cia.gov, but on the dark web the CIA’s web address
 18 is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.¹⁴ This prevents dark
 19 web marketplaces from being easily monitored by authorities or accessed by those not in the
 20 know.
 21
 22
 23

24 ¹¹ 17 C.F.R. § 248.201 (2013).

25 ¹² *Id.*

26 ¹³ *What Is the dark web?*, Experian, available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/>.

¹⁴ *Id.*

1 101. A sophisticated black market exists on the dark web where criminals can buy or
 2 sell malware, firearms, drugs, and frequently, and PII like the Private Information at issue here.¹⁵
 3 The digital character of Private Information stolen in data breaches lends itself to dark web
 4 transactions because it is immediately transmissible over the internet and the buyer and seller can
 5 retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical
 6 delivery address. Nefarious actors can readily purchase usernames and passwords for online
 7 streaming services, stolen financial information and account login credentials, and Social
 8 Security numbers, dates of birth, and medical information.¹⁶ As Microsoft warns “[t]he
 9 anonymity of the dark web lends itself well to those who would seek to do financial harm to
 10 others.”¹⁷

12 102. In addition, unencrypted and detailed Private Information may fall into the hands
 13 of companies that will use it for targeted marketing without the approval of Plaintiff and Class
 14 Members.

15 103. Unauthorized actors can easily access and misuse Plaintiff’s and Class Members’
 16 Private Information due to the Data Breach.

17 104. Because a person’s identity is akin to a puzzle with multiple data points, the more
 18 accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take
 19 on the victim’s identity, or to track the victim to attempt other hacking crimes against the
 20 individual to obtain more data to perfect a crime.
 21
 22

23 _____
 24 ¹⁵ *What is the dark web?* – Microsoft 365, available at <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web>.

25 ¹⁶ *Id.*; *What Is the dark web?*, Experian, available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/>.

26 ¹⁷ *What is the dark web?* – Microsoft 365, available at <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web>.

105. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as “social engineering” to obtain even more information about a victim’s identity, such as a person’s login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

106. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual’s Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don’t pay the bills, it damages your credit. You may not find out that someone is using your number until you’re turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.^[18]

107. What’s more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

¹⁸ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

108. Even then, new Social Security number may not be effective, as “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”¹⁹

109. Identity thieves can also use Social Security numbers to obtain a driver’s license or official identification card in the victim’s name but with the thief’s picture; use the victim’s name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim’s information. In addition, identity thieves may obtain a job using the victim’s Social Security number, rent a house or receive medical services in the victim’s name, and may even give the victim’s personal information to police during an arrest resulting in an arrest warrant issued in the victim’s name. And the Social Security Administration has warned that identity thieves can use an individual’s Social Security number to apply for credit lines.²⁰

110. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of “Fullz” packages.²¹

¹⁹ Brian Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited Dec. 27, 2024).

²⁰ *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), available at <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

²¹ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm> (last visited Dec. 27, 2024).

1 111. With “Fullz” packages, cyber-criminals can cross-reference two sources of
2 Private Information to marry unregulated data available elsewhere to criminally stolen data with
3 an astonishingly complete scope and degree of accuracy to assemble complete dossiers on
4 individuals.

5 112. The development of “Fullz” packages means here that the stolen Private
6 Information from the Data Breach can easily be used to link and identify it to Plaintiff’s and
7 Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers.
8 In other words, even if certain information such as emails, phone numbers, or credit card numbers
9 may not be included in the Private Information that was exfiltrated in the Data Breach, criminals
10 may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and
11 criminals (such as illegal and scam telemarketers) over and over.

12 113. Thus, even if certain information (such as driver’s license numbers) was not stolen
13 in the data breach, criminals can still easily create a comprehensive “Fullz” package.
14

15 114. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to
16 crooked operators and other criminals (like illegal and scam telemarketers).
17

18 115. The development of “Fullz” packages means that stolen Private Information from
19 the Data Breach can easily be used to link and identify it to Plaintiff’s and Class Members’ phone
20 numbers, email addresses, and other unregulated sources and identifiers. That is exactly what is
21 happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this
22 Court or a jury, to find that their stolen Private Information is being misused, and that such misuse
23 is traceable to the Data Breach.
24

25 116. Victims of identity theft can suffer from both direct and indirect financial losses.
26 According to a research study published by the Department of Justice,

1 A direct financial loss is the monetary amount the offender
 2 obtained from misusing the victim's account or personal
 3 information, including the estimated value of goods, services, or
 4 cash obtained. It includes both out-of-pocket loss and any losses
 5 that were reimbursed to the victim. An indirect loss includes any
 6 other monetary cost caused by the identity theft, such as legal fees,
 7 bounced checks, and other miscellaneous expenses that are not
 8 reimbursed (e.g., postage, phone calls, or notary fees). All indirect
 9 losses are included in the calculation of out-of-pocket loss.^[22]

10 117. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet
 11 Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar
 12 losses that year, resulting in more than \$3.5 billion in losses to individuals and business victims.²³

13 118. Further, according to the same report, "rapid reporting can help law enforcement
 14 stop fraudulent transactions before a victim loses the money for good."²⁴ Yet, Defendant failed
 15 to rapidly report to Plaintiff and Class Members that their Private Information was stolen.

16 119. Victims of identity theft also often suffer embarrassment, blackmail, or
 17 harassment in person or online, and/or experience financial losses resulting from fraudulently
 18 opened accounts or misuse of existing accounts.

19 120. In addition to out-of-pocket expenses that can exceed thousands of dollars and the
 20 emotional toll identity theft can take, some victims must spend a considerable time repairing the
 21 damage caused by the theft of their Private Information. Victims of new account identity theft
 22 will likely have to spend time correcting fraudulent information in their credit reports and
 23 continuously monitor their reports for future inaccuracies, close existing bank/credit accounts,
 24 open new ones, and dispute charges with creditors.

25 ²² Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity*
 26 *Theft*, 2018 I (2020) <https://bjs.ojp.gov/content/pub/pdf/vit18.pdf> (last accessed Jan. 23, 2024).

²³ See <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120>.

²⁴ *Id.*

121. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiff and Class Members will need to remain vigilant for years or even decades to come.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

122. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the asset of time has been lost.

123. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record

124. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate that harm.

125. Plaintiff and Class Members have spent time, and will spend additional time in the future, on a variety of prudent actions, such as placing “freezes” and “alerts” with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover.

126. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach,

1 including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud
 2 alert that lasts for seven years if someone steals their identity), reviewing their credit reports,
 3 contacting companies to remove fraudulent charges from their accounts, placing a credit freeze
 4 on their credit, and correcting their credit reports.²⁵

5 127. Once Private Information is exposed, there is virtually no way to ensure that the
 6 exposed information has been fully recovered or contained against future misuse. For this reason,
 7 Plaintiff and Class Members will need to maintain these heightened measures for years, and
 8 possibly their entire lives, as a result of Defendant's conduct that caused the Data Breach.
 9

10 ***Diminished Value of Private Information***

11 128. Private Information is a valuable property right.²⁶ Its value is axiomatic,
 12 considering the value of Big Data in corporate America and the consequences of cyber thefts
 13 include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond
 14 doubt that Private Information has considerable market value.
 15

16 129. For example, drug and medical device manufacturers, pharmacies, hospitals, and
 17 other healthcare service providers often purchase Private Information on the black market for the
 18 purpose of target-marketing their products and services to the physical maladies of the data
 19 breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to
 20 adjust their insureds' medical insurance premiums.
 21

22 130. Private Information can sell for as much as \$363 per record according to the

23 ²⁵ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last
 24 visited Feb. 26, 2024).

25 ²⁶ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable
 26 Information ("PRIVATE INFORMATION") Equals the "Value" of Financial Assets, 15 Rich.
 J.L. & Tech. 11, at *3-4 (2009) ("PRIVATE INFORMATION, which companies obtain at little
 cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional
 financial assets.") (citations omitted).

1 Infosec Institute.²⁷

2 131. An active and robust legitimate marketplace for Private Information also exists.
 3 In 2019, the data brokering industry was worth roughly \$200 billion.²⁸ In fact, the data
 4 marketplace is so sophisticated that consumers can actually sell their non-public information
 5 directly to a data broker who in turn aggregates the information and provides it to marketers or
 6 app developers.²⁹ Consumers who agree to provide their web browsing history to the Nielsen
 7 Corporation can receive up to \$50 a year.³⁰

9 132. As a result of the Data Breach, Plaintiff's and Class Members' Private
 10 Information, which has an inherent market value in both legitimate and dark markets, has been
 11 damaged and diminished in its value by its unauthorized and likely release onto the dark web,
 12 where holds significant value for the threat actors.

13 133. However, this transfer of value occurred without any consideration paid to
 14 Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the
 15 Private Information is now readily available, and the rarity of the data has been lost, thereby
 16 causing additional loss of value.

18 ***Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary***

19 134. To date, Defendant has done nothing to provide Plaintiff and Class Members with
 20 relief for the damages they have suffered due to the Data Breach. Defendant, which had a direct
 21

22 ²⁷ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015),
 23 [https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-](https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/)
 24 [market/](https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/).

25 ²⁸ Lazarus, D., *Shadowy data brokers make the most of their invisibility cloak*, LA TIMES (Nov.
 26 5, 2019), available at <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>.

²⁹ <https://datacoup.com/>.

³⁰ Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html>.

1 relationship with Plaintiff and Class Members, did not offer Data Breach victims even minimal
 2 compensation like temporary complimentary credit monitoring services, or even bother to notify
 3 its customers of their Private Information's unauthorized exposure in the Data Breach.

4 135. Given the type of targeted attack in this case and sophisticated criminal activity
 5 and the type of Private Information, there is a strong probability that the Private Information will
 6 be further published and on the black market/dark web for sale and purchase by criminals
 7 intending to utilize the it for identity theft crimes—*e.g.*, opening bank accounts in the victims'
 8 names to make purchases or to launder money, filing false tax returns, taking out loans or lines
 9 of credit, or filing false unemployment claims.

11 136. Such fraud may go undetected until debt collection calls commence months, or
 12 even years, later. An individual may not know that his or her Social Security number was used
 13 to file for unemployment benefits until law enforcement notifies the individual's employer of the
 14 suspected fraud. Fraudulent tax returns are typically discovered only when an individual's
 15 authentic tax return is rejected.

17 137. Furthermore, the information accessed and disseminated in the Data Breach is
 18 significantly more valuable than the loss of, for example, credit card information in a retailer data
 19 breach, where victims can easily cancel or close credit and debit card accounts.³¹ The information
 20 disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change
 21 (such as Social Security numbers).

23 138. Consequently, Plaintiff and Class Members are at a present and ongoing risk of
 24 fraud and identity theft for many years into the future, if not forever.

26 ³¹ See Jesse Damiani, *Your Social Security Number Costs \$4 On The dark web, New Report Finds*, FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.

139. The retail cost of credit monitoring and identity theft monitoring can cost \$200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Loss of Benefit of the Bargain

140. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain.

141. When agreeing to provide their Private Information, which was a condition precedent to obtain insurance and related services from Defendant, and paying Defendant, directly or indirectly, for these products and services, Plaintiff and Class Members as consumers understood and expected that they were, in part, paying a premium for services and data security to protect the Private Information they were required to provide.

142. In fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant.

V. PLAINTIFF'S EXPERIENCES AND INJURIES

143. As of condition of employment from Defendant, Plaintiff was required to supply Defendant and IMS with his Private Information, including but not limited to his name, contact information, date of birth, Social Security number, financial account number, personal address, and other sensitive information.

144. Plaintiff greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff diligently protects his Private Information and stores any

1 documents containing Private Information in a safe and secure location. He has never knowingly
2 transmitted unencrypted sensitive Private Information over the internet or any other unsecured
3 source.

4 145. Plaintiff would not have provided his Private Information to Defendant had he
5 known it would be kept using inadequate data security and vulnerable to a cyberattack.

6 146. At the time of the Data Breach—in or around November 2023—IMS retained
7 Plaintiff's Private Information in its network systems with inadequate data security, resulting in
8 Plaintiff's Private Information being accessed and exfiltrated by cybercriminals in the Data
9 Breach.
10

11 147. On or about November 15, 2024, Plaintiff received the Notice Letter informing
12 him that his Private Information was accessed and exposed to unauthorized third parties through
13 the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff's
14 sensitive Private Information, including his name and Social Security number.
15

16 148. Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach,
17 including but not limited to researching the Data Breach and reviewing credit reports and
18 financial account statements for any indications of actual or attempted identity theft or fraud,
19 signing up for credit monitoring services, changing passwords, and putting a hold on his credit
20 card account. Plaintiff now monitors his financial and credit statements multiple times a week
21 and has already spent hours dealing with the Data Breach, valuable time he otherwise would have
22 spent on other activities.
23

24 149. Plaintiff further anticipates spending considerable time and money on an ongoing
25 basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach,
26 Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for

1 years to come.

2 150. The risk of identity theft is impending and has materialized, as Plaintiff's and
3 Class Members' Private Information was targeted, accessed, misused, and disseminated on the
4 dark web following the Data Breach. Since the Data Breach, Plaintiff has received an alert from
5 a commercially available product that his Private Information was found on the dark web. He
6 also has experienced a spike in spam and fraudulent calls and emails since the Data Breach.

7 151. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has
8 been compounded by the fact that Defendant have still not fully informed him of key details
9 about the Data Breach's occurrence or the information stolen. Plaintiff has suffered and continues
10 to suffer anxiety and fear about the genuine and materialized risk that he will be the victim of
11 identity theft due to his Private Information's exposure in the Data Breach.

12 152. Moreover, following the Data Breach, Plaintiff has experienced suspicious spam
13 calls, texts, and emails using the Private Information exposed in the Data Breach, giving rise to
14 further anxiety and stress that his Private Information is now in the hands of bad actors.

15 VI. CLASS ACTION ALLEGATIONS

16 153. Plaintiff bring this nationwide class action on behalf of himself and others
17 similarly situated pursuant to Federal Rule of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

18 154. Plaintiff proposes the following nationwide class definition, subject to
19 amendment based on information obtained through discovery:

20 All persons in the United States whose Private Information was
21 provided to Defendant and compromised in the Data Breach,
22 including all persons who received a Notice Letter sent on
23 Defendant's behalf ("Class").

24 155. Excluded from the Class are the following individuals and/or entities: Defendant
25 and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which
26

1 Defendant has a controlling interest; all individuals who make a timely election to be excluded
 2 from this proceeding using the correct protocol for opting out; any and all federal, state or local
 3 governments, including but not limited to their departments, agencies, divisions, bureaus, boards,
 4 sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this
 5 litigation, as well as their immediate family members.

6 156. Plaintiff reserves the right to modify or amend the definition of the proposed Class
 7 before the Court determines whether certification is appropriate.
 8

9 157. **Numerosity:** The Class is so numerous that joinder of all members is
 10 impracticable. While the exact number of Class Members is unknown to Plaintiff at this time,
 11 upon information and belief, there are at least thousands of individuals affected, making joinder
 12 of all members of the Class impractical.

13 158. **Commonality:** Questions of law and fact common to the Class exist and
 14 predominate over any questions affecting only individual Class Members. These include:
 15

- 16 a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and
 17 Class Members' Private Information;
- 18 b. Whether and to what extent Defendant had a duty to protect the Private Information of
 19 Plaintiff and Class Members;
- 20 c. Whether Defendant had a duty not to disclose the Private Information of Plaintiff and
 21 Class Members to unauthorized third parties;
- 22 d. Whether Defendant had a duty not to use the Private Information of Plaintiff and Class
 23 Members for non-business purposes;
- 24 e. Whether Defendant had a duty to supervise its vendors' data security for Private
 25 Information;
 26

- 1 f. Whether Defendant knew or should have known of the data security vulnerabilities
- 2 that allowed the Data Breach to occur;
- 3 g. Whether Defendant knew or should have known of the risks to Plaintiff's and Class
- 4 Members' Private Information in IMS's custody;
- 5 h. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff
- 6 and Class Members;
- 7 i. When Defendant actually learned of the Data Breach;
- 8 j. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class
- 9 Members their Private Information had been compromised;
- 10 k. Whether Defendant violated data breach notification laws by failing to promptly notify
- 11 Plaintiff and Class Members that their Private Information had been compromised;
- 12 l. Whether Defendant's conduct violated the FTC Act;
- 13 m. Whether Defendant failed to implement and maintain reasonable security procedures
- 14 and practices appropriate to the nature and scope of the Private Information
- 15 compromised in the Data Breach;
- 16 n. Whether Defendant and/or IMS adequately addressed and remedied the vulnerabilities
- 17 that permitted the Data Breach to occur;
- 18 o. Whether Defendant engaged in unfair, unlawful, or deceptive practice by failing to
- 19 safeguard the Private Information of Plaintiff and Class Members;
- 20 p. Whether Defendant engaged in unfair, unlawful, or deceptive practice by concealing
- 21 and/or misrepresenting its and its vendors' data security processes and vulnerabilities;
- 22 q. Whether Defendant were unjustly enriched by failing to provide adequate security for
- 23 Plaintiff's and Class Members' Private Information;
- 24
- 25
- 26

- 1 r. Whether Plaintiff and Class Members are entitled to actual, consequential, nominal,
2 statutory, and/or punitive damages as a result of Defendant's wrongful conduct;
3 s. Whether Plaintiff and Class Members are entitled to restitution as a result of
4 Defendant's wrongful conduct; and
5 t. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the
6 imminent and currently ongoing harm the Data Breach caused.

7
8 159. **Typicality:** Plaintiff's claims are typical of other Class Members' claims because
9 Plaintiff and Class Members were subject to the same unlawful conduct as alleged herein, and
10 were damaged in the same way. Plaintiff's Private Information provided to Defendant and
11 through Defendant, to IMS, and was compromised due to the Data Breach. Plaintiff's damages
12 and injuries are akin to those of other Class Members and Plaintiff seeks relief consistent with
13 the relief of the Class.

14
15 160. **Adequacy:** Plaintiff is an adequate representative of the Class because he is a
16 member of the Nationwide Class and committed to pursuing this matter against Defendant to
17 obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel
18 are competent and experienced in litigating class actions, including extensive experience in data
19 breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly
20 and adequately protect the interests of the Class.

21
22 161. **Superiority:** A class action is superior to any other available means for the fair
23 and efficient adjudication of this controversy, and no unusual difficulties are likely to be
24 encountered in the management of this class action. The purpose of the class action mechanism
25 is to permit litigation against wrongdoers even when damages to Plaintiff and Class Members
26 may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and

1 Class Members are relatively small compared to the burden and expense required to individually
2 litigate their claims against Defendant, and thus, individual litigation to redress Defendant's
3 wrongful conduct would be impracticable. Individual litigation by each Class Member would
4 also strain the court system. Individual litigation creates the potential for inconsistent or
5 contradictory judgments and increases the delay and expense to all parties and the court system.
6 By contrast, the class action device presents far fewer management difficulties and provides the
7 benefits of a single adjudication, economies of scale, and comprehensive supervision by a single
8 court.
9

10 162. **Manageability:** The litigation of the class claims alleged herein is manageable.
11 Defendant's uniform conduct, the consistent provisions of the relevant laws, and the
12 ascertainable identities of Class Members demonstrates there would be no significant
13 manageability problems with prosecuting this lawsuit as a class action. Adequate notice can be
14 given to Class Members directly using information maintained in Defendant's and/or IMS's
15 records.
16

17 163. **Ascertainability:** All members of the proposed Class are readily ascertainable.
18 The Class is defined by reference to objective criteria, and there is an administratively feasible
19 mechanism to determine who fits within the Class. Defendant has access to information regarding
20 the individuals affected by the Data Breach, and IMS has already provided notifications to some
21 or all of those people on Defendant's behalf. Using this information, the members of the Class
22 can be identified, and their contact information ascertained for purposes of providing notice.
23

24 164. **Particular Issues:** Particular issues are appropriate for certification under Rule
25 23(c)(4) because such claims present only particular, common issues, the resolution of which
26 would advance the disposition of this matter and the parties' interests therein. Such particular

1 issues include, but are not limited to the following:

- 2 a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due
- 3 care in collecting, storing, using, and safeguarding their Private Information;
- 4 b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise
- 5 due care in collecting, storing, using, and safeguarding their Private Information;
- 6 c. Whether Defendant failed to comply with its own policies and applicable laws,
- 7 regulations, and industry standards relating to data security;
- 8 d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff
- 9 and Class Members on the other, and the terms of that implied contract;
- 10 e. Whether Defendant breached the implied contract;
- 11 f. Whether Defendant adequately and accurately informed Plaintiff and Class Members
- 12 their Private Information had been compromised;
- 13 g. Whether Defendant failed to implement and maintain reasonable security procedures
- 14 and practices appropriate to the nature and scope of the information compromised in
- 15 the Data Breach;
- 16 h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to
- 17 safeguard the Private Information of Plaintiff and Class Members; and
- 18 i. Whether Class Members are entitled to actual, consequential, statutory, and/or
- 19 nominal damages, and/or injunctive relief as a result of Defendant's wrongful
- 20 conduct.
- 21
- 22
- 23

24 165. **Policies Generally Applicable to the Class:** Finally, class certification is also
 25 appropriate under Rule 23(b)(2) and (c). The Class is appropriate for certification because
 26 Defendant has acted or refused to act on grounds generally applicable to the Class, thereby

1 requiring the Court's imposition of uniform relief to ensure compatible standards of conduct
 2 toward Class Members and making final injunctive relief appropriate with respect to each of the
 3 Class as a whole. Defendant's policies challenged herein apply to and affect Class Members
 4 uniformly, and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect
 5 to the Class as a whole, not on facts or law applicable only to Plaintiff.

6
 7 166. Defendant, through uniform conduct, acted or refused to act on grounds generally
 8 applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the
 9 Class as a whole, including without limitation the following:

- 10 a. Ordering Defendant to provide lifetime credit monitoring and identity theft insurance
 11 to Plaintiff and Class Members; and
- 12 b. Ordering that, to comply with Defendant's explicit or implicit contractual obligations
 13 and duties of care, Defendant must implement and maintain, and must require its
 14 vendors handling Private Information to implement and maintain, reasonable security
 15 and monitoring measures, including, but not limited to the following:
 - 16 i. prohibiting Defendant from engaging in the wrongful and unlawful acts alleged
 17 herein;
 - 18 ii. requiring Defendant to obligate and ensure its vendors protect, including
 19 through encryption, all data collected by Defendant and shared with its vendors
 20 through the course of business in accordance with all applicable regulations,
 21 industry standards, and federal, state or local laws;
 - 22 iii. requiring Defendant to implement and maintain a comprehensive Information
 23 Security Program designed to protect the confidentiality and integrity of
 24 Plaintiff's and Class Members' Private Information;

- iv. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's vendors' systems on a periodic basis;
- v. prohibiting Defendant from allowing its vendors to maintain Private Information on a cloud-based database until proper safeguards and processes are ensured;
- vi. requiring Defendant to obligate its vendors to segment data by creating firewalls and access controls so that, if one area of their network is compromised, hackers cannot gain access to other portions of their systems;
- vii. requiring Defendant to obligate its vendors to conduct regular database scanning and securing checks;
- viii. requiring Defendant to obligate its vendors to monitor ingress and egress of all network traffic;
- ix. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor its vendors' networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;
- x. requiring Defendant to meaningfully educate all Class Members about the threats that they because of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves; and
- xi. incidental retrospective relief, including but not limited to restitution.

VII. CLAIMS FOR RELIEF

COUNT I: NEGLIGENCE
(On behalf of Plaintiff and the Class)

167. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 166 above as if fully set forth herein.

168. Defendant required Plaintiff and Class Members to submit, directly or indirectly, personal, confidential Private Information to Defendant and its vendor IMS as a condition of employment.

169. Plaintiff and Class Members provided certain Private Information to Defendant and, through Defendant, to IMS, including their names, date of birth, financial account number, personal address, and Social Security numbers.

170. Defendant had full knowledge of the sensitivity of the Private Information to which it was entrusted, and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed to unauthorized persons.

171. Defendant had duties to Plaintiff and each Class Member to exercise reasonable care in holding, using, sharing, safeguarding, and protecting their Private Information, including requiring and ensuring its vendors handling Private Information had reasonable and appropriate data security measures and policies in place to do so.

172. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices by Defendant or its service provider IMS.

173. Plaintiff and Class Members had no ability to protect their Private Information in Defendant's care or IMS's possession.

174. By collecting and storing Plaintiff's and Class Members' Private Information, Defendant had a duty of care to use reasonable means to secure and safeguard it, to prevent

1 disclosure of the information, and to safeguard the Private Information from theft.

2 175. Defendant's duty of care obligated it to require and ensure that its vendor IMS
3 provided data security data security consistent with industry standards and legal and regulatory
4 requirements, and that IMS's systems and networks and the personnel responsible for them
5 adequately protected Plaintiff's and Class Members' Private Information.

6 176. Defendant's duty of care further obligated it to ensure its vendor IMS's processes
7 to detect compromises of Private Information were sufficient.
8

9 177. Defendant was able to ensure IMS's systems and data security procedures were
10 sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a
11 cybersecurity event like this Data Breach, whereas Plaintiff and Class Members were not.

12 178. Defendant had a duty to employ reasonable security measures under Section 5 of
13 the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce,"
14 including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable
15 measures to protect confidential data.
16

17 179. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide
18 adequate computer systems and data security practices to safeguard Plaintiff's and Class
19 Members' PHI.

20 180. Defendant breached their duties to Plaintiff and Class Members under the FTC
21 Act by failing to require, through contract or oversight, that its service provider IMS provided
22 fair, reasonable, and adequate computer systems and data security practices to safeguard
23 Plaintiff's and Class Members' Private Information, by failing to ensure the Private Information
24 on IMS's system was encrypted and timely deleted when no longer needed, and by failing to
25 provide notice to Plaintiff and Class Members of the Data Breach until nearly a year after it was
26

1 discovered.

2 181. Defendant's violations of the FTC Act as described herein directly caused and/or
3 were a substantial factor in the Data Breach and resulting injuries to Plaintiff and Class Members.

4 182. Plaintiff and Class Members are within the class of persons the FTC Act was
5 intended to protect.

6 183. The type of harm that resulted from the Data Breach was the type of harm the
7 FTC Act was intended to guard against.

8 184. Defendant's duty to use reasonable care in protecting Plaintiff's and Class
9 Members' Private Information arose not only as a result of the statutes and regulations described
10 above, but also because Defendant is bound by industry standards to secure such Private
11 Information.
12

13 185. Defendant breached its duties and was negligent by failing to use reasonable
14 measures to protect Plaintiff's and Class Members' Private Information from unauthorized
15 disclosure in the Data Breach. The specific negligent acts and omissions committed by Defendant
16 include, but are not limited to, the following:
17

- 18 a. Failing to require and periodically ensure that its vendor IMS adopted, implemented,
19 and maintain adequate security measures to safeguard Plaintiff's and Class Members'
20 Private Information;
21 b. Failing to adequately monitor the security of IMS's information technology networks
22 and systems;
23 c. Failure to require and periodically ensure that IMS's network systems had plans in
24 place to maintain reasonable data security safeguards;
25 d. Allowing unauthorized access to Plaintiff's and Class Members' Private Information;
26

1 and

- 2 e. Failing to timely notify Plaintiff and Class Members about the Data Breach so that
3 they could take appropriate steps to mitigate the potential for identity theft and other
4 damages.

5 186. But for Defendant's wrongful and negligent breaches of its duties owed to
6 Plaintiff and Class Members, the Data Breach would not have occurred or at least would have
7 been mitigated, Plaintiff's and Class Members' Private Information would not have been
8 compromised, and Plaintiff's and Class Members' injuries would have been avoided.
9

10 187. It was foreseeable that Defendant's failures to use reasonable measures to protect
11 Plaintiff's and Class Members' Private Information would injure Plaintiff and Class Members.
12 Further, the breach of security was reasonably foreseeable to Defendant given the known high
13 frequency of cyber-attacks and data breaches in Defendant's industry.
14

15 188. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and
16 Class Members' Private Information would cause them one or more types of injuries.

17 189. As a direct and proximate result of Defendant's negligence, Plaintiff and Class
18 Members have suffered and will suffer injuries and damages, including but not limited to (a)
19 invasion of privacy; (b) lost or diminished value of their Private Information; (c) actual identity
20 theft and fraud; (d) lost opportunity costs associated with attempting to mitigate the actual
21 consequences of the Data Breach, including but not limited to lost time; (e) loss of benefit of
22 their bargain; and (f) the continued and certainly increased risk to their Private Information,
23 which remains (i) unencrypted and available for unauthorized third parties to access and abuse;
24 and (ii) in Defendant's control and IMS's possession and subject to further unauthorized
25 disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect
26

1 it.

2 190. As a direct and proximate result of Defendant's negligence, Plaintiff and Class
3 Members have suffered and will continue to suffer other forms of injuries and/or harm, including,
4 but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-
5 economic losses.

6 191. Plaintiff and Class Members are entitled to damages, including compensatory,
7 punitive, and nominal damages, in an amount to be proven at trial.

9 **COUNT II: VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT,**

10 **RCW 19.86**

(On behalf of Plaintiff and the Class)

11 192. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 166
12 above as if fully set forth herein

13 193. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA")
14 prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as
15 those terms are described by the CPA and relevant case law.

16 194. Defendant is a "person" as described in RCW 19.86.010(1).

17 195. Defendant engages in "trade" and "commerce" as described in RCW
18 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly
19 affecting the people of the state of Washington.

20 196. By virtue of the above-described wrongful actions, inaction, omissions, and
21 want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged
22 in unlawful, unfair, and fraudulent practices within the meaning of, and in violation of, the
23 CPA, in that Defendant's practices were injurious to the public interest because they injured
24
25
26

1 other persons, had the capacity to injure other persons, and have the capacity to injure other
2 persons.

3 197. Defendant's failure to safeguard the Private Information exposed in the Data
4 Breach constitutes an unfair act that offends public policy.

5 198. Defendant's failure to safeguard the Private Information compromised in the
6 Data Breach caused substantial injury to Plaintiff and Class Members. Defendant's failure is
7 not outweighed by any countervailing benefits to consumers or competitors, and it was not
8 reasonably avoidable by consumers.
9

10 199. Defendant's failure to safeguard the Private Information disclosed in the Data
11 Breach, and its failure to provide timely and complete notice of that Data Breach to the victims,
12 is unfair because these acts and practices are immoral, unethical, oppressive, and/or
13 unscrupulous.

14 200. In the course of conducting its business, Defendant committed "unfair or
15 deceptive acts or practices" by, inter alia, knowingly failing to design, adopt, implement,
16 control, direct, oversee, manage, monitor, and audit appropriate data security processes for its
17 vendors; its failure to develop or oversee controls, policies, procedures, protocols, and software
18 and hardware systems to safeguard and protect Plaintiff's and Class Members' PII; and
19 violating the common law in the process. Plaintiff and Class Members reserve the right to
20 allege other violations of law by Defendant constituting other unlawful business acts or
21 practices. As described above, Defendant's wrongful actions, inaction, omissions, and want of
22 ordinary care are ongoing and continue to this date.
23
24

25 201. Defendant also violated the CPA by failing to timely notify, and by concealing
26 from Plaintiff and Class Members, information regarding the unauthorized release and

1 disclosure of their Private Information. If Plaintiff and Class Members had been notified in an
2 appropriate fashion, and had the information not been hidden from them, they could have taken
3 precautions to safeguard and protect their Private Information.

4 202. The gravity of Defendant's wrongful conduct outweighs any alleged benefits
5 attributable to such conduct. There were reasonably available alternatives to further
6 Defendant's legitimate business interests other than engaging in the above-described wrongful
7 conduct.
8

9 203. Defendant's unfair or deceptive acts or practices occurred in its trade or
10 business and have injured and are capable of injuring a substantial portion of the public.
11 Defendant's general course of conduct as alleged herein is injurious to the public interest, and
12 the acts complained of herein are ongoing and/or have a substantial likelihood of being
13 repeated.
14

15 204. As a direct and proximate result of Defendant's above-described wrongful
16 actions, inaction, omissions, and want of ordinary care that directly and proximately caused the
17 Data Breach and its violations of the CPA, Plaintiff and Class Members have suffered, and will
18 continue to suffer, economic damages and other injury and actual harm in the form of, inter
19 alia, (1) an imminent, immediate, and continuing increased risk of identity theft and identity
20 fraud—risks justifying expenditures for protective and remedial services for which they are
21 entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of their PII;
22 (4) deprivation of the value of their PII, for which there is a well-established national and
23 international market; and/or (5) the financial and temporal costs of monitoring credit,
24 monitoring financial accounts, and mitigating damages.
25
26

1 205. Unless restrained and enjoined, Defendant will continue to engage in the
 2 above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on
 3 behalf of himself and the Class, seek restitution and an injunction prohibiting Defendant from
 4 continuing such wrongful conduct, and requiring Defendant to design, adopt, implement,
 5 control, direct, oversee, manage, monitor and audit appropriate data security processes,
 6 controls, policies, procedures protocols, and software and hardware systems to safeguard and
 7 protect the PII entrusted to it.
 8

9 206. Plaintiff, on behalf of himself and Class Members, also seeks to recover actual
 10 damages sustained by each Class Member together with the costs of the suit, including reasonable
 11 attorneys' fees. In addition, Plaintiff, on behalf of himself and Class Members, requests that this
 12 Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each
 13 Class Member by three times the actual damages sustained, not to exceed \$25,000.00 per Class
 14 Member.
 15

COUNT III: BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

17 207. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 166 above
 18 as if fully set forth herein.
 19

20 208. Defendant required Plaintiff and Class Members to provide and entrust their
 21 Private Information to Defendant as a condition of employment from Defendant.

22 209. When Plaintiff and Class Members provided their Private Information to
 23 Defendant, they entered into implied contracts with Defendant pursuant to which Defendant
 24 agreed to safeguard and protect such Private Information and to timely and accurately notify
 25 Plaintiff and Class Members if and when their Private Information was breached and
 26 compromised.

1 210. Specifically, Plaintiff and Class Members entered into valid and enforceable
2 implied contracts with Defendant when they agreed to provide their Private Information and/or
3 payment to Defendant.

4 211. The valid and enforceable implied contracts that Plaintiff and Class Members
5 entered into with Defendant included Defendant's promises to protect Private Information it
6 collected from Plaintiff and Class Members, or created on its own, from unauthorized disclosures.
7 Plaintiff and Class Members provided this Private Information in reliance on Defendant's
8 promises.
9

10 212. Under the implied contracts, Defendant promised and was obligated to (a) provide
11 insurance and/or benefits products and services to Plaintiff and Class Members; and (b) protect
12 Plaintiff's and Class Members' Private Information provided to obtain such services and/or
13 created in connection therewith. In exchange, Plaintiff and Class Members agreed to provide
14 Defendant with payment and their Private Information.
15

16 213. Defendant promised and warranted to Plaintiff and Class Members, including
17 through its public-facing Privacy Notice identified above, to maintain the privacy and
18 confidentiality of the Private Information it collected from Plaintiff and Class Members and to
19 keep such information safeguarded against unauthorized access and disclosure.

20 214. Defendant's adequate protection of Plaintiff's and Class Members' Private
21 Information was a material aspect of these implied contracts with Defendant.
22

23 215. Defendant solicited and invited Plaintiff and Class Members to provide their
24 Private Information as part of Defendant's regular business practices. Plaintiff and Class
25 Members accepted Defendant's offers and provided their Private Information to Defendant.

26 216. In entering into such implied contracts, Plaintiff and Class Members reasonably

1 believed and expected that Defendant's data security practices complied with industry standards
2 and relevant laws and regulations, including the FTC Act.

3 217. Plaintiff and Class Members who contracted with Defendant for insurance and/or
4 benefit products and services and provided their Private Information to Defendant reasonably
5 believed and expected that Defendant would adequately employ adequate data security to protect
6 that Private Information. Defendant failed to do so.

7
8 218. A meeting of the minds occurred when Plaintiff and Class Members agreed to,
9 and did, provide their Private Information to Defendant and agreed Defendant would, among
10 other things, protect their Private Information.

11 219. Plaintiff and Class Members performed their obligations under the contracts when
12 they provided their Private Information and/or payment to Defendant.

13 220. Defendant materially breached its contractual obligations to protect the Private
14 Information it required Plaintiff and Class Members to provide when that Private Information
15 was unauthorizedly disclosed in the Data Breach due to Defendant's inadequate data security
16 measures and procedures.

17
18 221. Defendant materially breached its contractual obligations to deal in good faith
19 with Plaintiff and Class Members when it failed to take adequate precautions to prevent the Data
20 Breach and failed to promptly notify Plaintiff and Class Members of the Data Breach.

21 222. Defendant materially breached the terms of its implied contracts, including but
22 not limited to by failing to comply with industry standards or the standards of conduct embodied
23 in statutes like Section 5 of the FTC Act, by failing to otherwise protect Plaintiff's and Class
24 Members' Private Information, and/or by failing to prevent the same data security failures by its
25 vendor IMS that handled Private Information, as set forth *supra*.
26

1 223. The Data Breach was a reasonably foreseeable consequence of Defendant's
2 conduct, by acts of omission or commission, in breach of these implied contracts with Plaintiff
3 and Class Members.

4 224. As a result of Defendant's failure to fulfill the data security protections promised
5 in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargains
6 with Defendant, and instead received services of a diminished value compared to that described
7 in the implied contracts. Plaintiff and Class Members were therefore damaged in an amount at
8 least equal to the difference in the value of the services with data security protection they paid
9 for and that which they received.

11 225. Had Defendant disclosed that its data security procedures were inadequate or that
12 it and its vendor did not adhere to industry-standard for cybersecurity, neither Plaintiff, Class
13 Members, nor any reasonable person would have contracted with Defendant.

14 226. Plaintiff and Class Members would not have provided and entrusted their Private
15 Information to Defendant in the absence of the implied contracts between them and Defendant.

16 227. Plaintiff and Class Members fully performed their obligations under the implied
17 contracts with Defendant.

18 228. Defendant breached the implied contracts it made with Plaintiff and Class
19 Members by failing to safeguard and protect their Private Information and by failing to provide
20 timely or adequate notice that their Private Information was compromised in and due to the Data
21 Breach.

22 229. As a direct and proximate result of Defendant's breach of its implied contracts
23 with Plaintiff and Class Members and the attendant Data Breach, Plaintiff and Class Members
24 have suffered injuries and damages as set forth herein and have been irreparably harmed, as well
25
26

1 as suffering and the loss of the benefit of the bargain they struck with Defendant.

2 230. Plaintiff and Class Members are entitled to damages, including compensatory,
3 punitive, and/or nominal damages, and/or restitution, in an amount to be proven at trial.

4 231. Plaintiff and Class Members are also entitled to injunctive relief requiring
5 Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring procedures; (b)
6 conduct annual audits of its vendor's data security systems and monitoring procedures; and (c)
7 provide adequate lifetime credit monitoring to all Class Members.
8

9 **COUNT IV: INVASION OF PRIVACY/INTRUSION UPON SECLUSION**
10 **(On behalf of Plaintiff and the Class)**

11 232. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 166 above
12 as if fully set forth herein.

13 233. Plaintiff and Class Members had a legitimate expectation of privacy to their
14 Private Information and were entitled to Defendant's protection of this Private Information in its
15 control against disclosure to unauthorized third parties.

16 234. Defendant owed a duty to its customers, including Plaintiff and Class Members,
17 to keep their Private Information confidential and secure.

18 235. Defendant failed to protect Plaintiff's and Class Members' Private Information
19 and instead caused it to be accessed and exposed to unauthorized persons, cybercriminals, which
20 has already made the Private Information publicly available and disseminated it to thousands of
21 people, including through publishing the data on its dark web leak site, where cybercriminals go
22 to find their next identity theft and extortion victims.
23

24 236. Defendant allowed unauthorized third parties access to and examination of the
25 Private Information of Plaintiff and Class Members, by way of Defendant's failure to protect the
26 Private Information through reasonable data security measures.

1 237. The unauthorized release to, custody of, and examination by unauthorized third
2 parties of the Private Information of Plaintiff and Class Members is highly offensive to a
3 reasonable person and represents an intrusion upon Plaintiff's and Class Members' seclusion as
4 well as a public disclosure of private facts.

5 238. The intrusion was into a place or thing, which was private and is entitled to be
6 private. Plaintiff and Class Members disclosed their Private Information to Defendant as a
7 condition of and in exchange for receiving insurance and/or benefits products and services, but
8 privately with an intention that the Private Information would be kept confidential and protected
9 from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that
10 such information would be kept private and would not be disclosed without their authorization.

11 239. Subsequent to the intrusion, Defendant permitted Plaintiff's and Class Members'
12 data to be published online to countless cybercriminals whose mission is to misuse such
13 information, including through identity theft and extortion.
14

15 240. The Data Breach constitutes an intentional or reckless interference by Defendant
16 with Plaintiff's and Class Members' interests in solitude or seclusion, as to their persons or as to
17 their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.
18

19 241. Defendant acted with a knowing state of mind when it permitted the Data Breach
20 to occur, because it had actual knowledge that its diligence and oversight of its vendors'
21 information security practices were inadequate and insufficient to protect Plaintiff' and Class
22 Members' Private Information from unauthorized disclosure.
23

24 242. Defendant acted with reckless disregard for Plaintiff' and Class Members'
25 privacy when it caused their Private Information to be shared, used, and stored by IMS without
26 adequate protections, including encryption, allowing cybercriminals to access and take Plaintiff's

1 and Class Members' Private Information in the Data Breach.

2 243. Defendant was aware of the potential of a data breach and failed to adequately vet,
3 audit, or oversee its vendor IMS's network systems or implement appropriate policies to prevent
4 the unauthorized release of Plaintiff' and Class Members' Private Information to cybercriminals.

5 244. Because Defendant acted with this knowing state of mind, it had notice and knew
6 that its inadequate and insufficient information security practices would cause injury and harm to
7 Plaintiff and Class Members.

8 245. As a direct and proximate result of Defendant's acts and omissions set forth above,
9 Plaintiff' and Class Members' Private Information was disclosed to third parties without
10 authorization, causing Plaintiff and Class Members to suffer injuries and damages including,
11 without limitation, (a) invasion of privacy; (b) lost or diminished value of their Private
12 Information; (c) out-of-pocket and lost opportunity costs associated with attempting to mitigate
13 the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of
14 benefit of the bargain; and (e) the continued and certainly increased risk to their Private
15 Information, which remains in Defendant's control and its vendors' possession in unencrypted
16 form and subject to further unauthorized disclosures, so long as Defendant fails to undertake
17 appropriate and adequate measures to protect it.

18 246. Unless and until enjoined and restrained by order of this Court, Defendant's
19 wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class
20 Members in that the Private Information maintained by Defendant can be viewed, distributed,
21 and used by unauthorized persons for years to come. Plaintiff and Class Members have no
22 adequate remedy at law for the injuries in that a judgment for monetary damages will not end the
23 invasion of privacy for Plaintiff and Class Members.
24
25
26

COUNT V: UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class)

247. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 166 above as if fully set forth herein.

248. This count is brought in the alternative to the breach of implied contract count above.

249. Plaintiff and Class Members conferred a monetary benefit on Defendant in connection with employment, specifically providing Defendant, with their PII.

250. Defendant required Plaintiff's and Class Members' Private Information to conduct and facilitate its business and generate revenue, which it could not do without collecting, using, and sharing with IMS Plaintiff's and Class Members' Private Information.

251. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiff's retained data and use Plaintiff's and Class Members' PII for business purposes.

252. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by hiring vendors with cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

253. Defendant failed to provide reasonable security, safeguards, and protections to the

1 Private Information of Plaintiff and Class Members, and as a result, Defendant was overpaid.

2 254. Under principles of equity and good conscience, Defendant should not be
3 permitted to retain the money because it failed to provide adequate safeguards and security
4 measures to protect Plaintiff's and Class Members' Private Information, which Plaintiff and
5 Class Members paid for but did not receive.

6 255. Defendant wrongfully accepted and retained these benefits—employment and
7 Plaintiff's and Class Members' Private Information—and was enriched to the detriment of
8 Plaintiff and Class Members.

9 256. Defendant's enrichment at Plaintiff's and Class Members' expense is unjust.

10 257. As a result of Defendant's wrongful conduct and resulting unjust enrichment,
11 Plaintiff and Class Members are entitled to restitution and disgorgement of profits, benefits, and
12 other compensation obtained by Defendant, plus reasonable attorneys' fees and costs.
13

14 **COUNT VI: DECLARATORY JUDGMENT**
15 **(On behalf of Plaintiff and the Class)**

16 258. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 166 above
17 as if fully set forth herein.

18 259. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is
19 authorized to enter a judgment declaring the rights and legal relations of the parties and to grant
20 further necessary supplemental relief. The Court has broad authority to restrain acts, such as those
21 alleged herein, which are tortious and unlawful.
22

23 260. In the fallout of the Data Breach, a controversy has arisen about Defendant's
24 duties to use reasonable data security for the Private Information it collects, uses, shares, and
25 maintains.
26

261. On information and belief, Defendant's actions were—and *still* are—inadequate

1 and unreasonable. Plaintiff and Class Members continue to suffer injuries from the ongoing threat
2 of fraud and identity theft due to Defendant's inadequate data security measures.

3 262. Given its authority under the Declaratory Judgment Act, this Court should enter a
4 judgment declaring as follows:

- 5 a. Defendant owed—and continue to owe—a legal duty to use reasonable data security
6 to secure the Private Information entrusted to it;
- 7 b. Defendant has a duty to notify impacted individuals of the Data Breach under the
8 common law and Section 5 of the FTC Act;
- 9 c. Defendant breached, and continue to breach, its duties by failing to use reasonable
10 measures to protect the Private Information entrusted to it from unauthorized access,
11 use, and disclosure; and
- 12 d. Defendant's breaches of its duties caused—and continues to cause—injuries to
13 Plaintiff and Class Members.

14 263. The Court should also issue injunctive relief requiring Defendant to use adequate
15 security consistent with industry standards to protect the Private Information entrusted to it.

16 264. That Defendant's service provider was previously the target of one of a
17 devastating data breach, yet Defendant still refused to act proactively to prevent the exposure of
18 thousands of individuals' Private Information in this Data Breach through improved data security
19 vetting, auditing, and supervision measures, like thorough due diligence and oversight of its
20 vendors handling Private Information, highlights the need for an injunction here—lest Defendant
21 continue to skimp on cybersecurity to augment its own profits while leaving individuals like
22 Plaintiff and Class Members to suffer the consequences.

23 265. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable
24
25
26

1 injuries and lack an adequate legal remedy if Defendant's vendor(s) experiences another data
 2 breach. And if another breach occurs, Plaintiff and Class Members will lack an adequate remedy
 3 at law because many of the resulting injuries are not readily quantified in full, and they will be
 4 forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages,
 5 while warranted for out-of-pocket damages and other legally quantifiable and provable damages,
 6 cannot cover the full extent of Plaintiff's and Class Members' injuries.

7
 8 266. If an injunction is not issued, the resulting hardship to Plaintiff and Class
 9 Members far exceeds the minimal hardship that Defendant could experience if an injunction is
 10 issued.

11 267. An injunction would benefit the public by preventing another data breach—thus
 12 preventing further injuries to Plaintiff, Class Members, and the public at large.

13 **VIII. PRAYER FOR RELIEF**

14 **WHEREFORE**, Plaintiff, on behalf of himself and all others similarly situated, prays for
 15 judgment as follows:
 16

17 A. An Order certifying this case as a class action on behalf of Plaintiff and the
 18 proposed Class, appointing Plaintiff as class representative, and appointing his counsel to
 19 represent the Class;

20 B. Awarding Plaintiff and the Class damages that include applicable compensatory,
 21 actual, statutory, nominal, exemplary, treble, and punitive damages, as allowed by law;

22 C. Awarding restitution and damages to Plaintiff and the Class in an amount to be
 23 determined at trial;

24 D. Awarding declaratory and other equitable relief as is necessary to protect the
 25 interests of Plaintiff and the Class;
 26

1 E. Awarding injunctive relief in the form of additional technical and administrative
2 cybersecurity controls as is necessary to protect the interests of Plaintiff and the Class;

3 F. Enjoining Defendant from further deceptive practices and making untrue
4 statements about its data security, the Data Breach, and the transmitted Private Information;

5 G. Awarding attorneys' fees and costs, as allowed by law, including under the
6 Washington Consumer Protection Act;

7 H. Awarding prejudgment and post-judgment interest, as provided by law; and

8 I. Awarding such further relief to which Plaintiff and the Class are entitled.
9

10 **IX. DEMAND FOR JURY TRIAL**

11 Plaintiff demands a trial by jury on all issues to triable.

12 Dated: December 30, 2024 Respectfully submitted,

13
14 TOUSLEY BRAIN STEPHENS PLLC

15
16 By: /s/ Kaleigh N. Boyd

17 Kaleigh N. Boyd, WSBA No. 52684
18 **TOUSLEY BRAIN STEPHENS PLLC**
19 1200 Fifth Avenue, Ste. 1700
20 Seattle, WA 98101-3147
Telephone (206) 682-5600
Facsimile (206) 682-2992
Email: kboyd@tousley.com

21 Gary Klinger*
22 **MILBERG LAW FIRM**
23 800 S. Gay Street, Suite 1100
24 Knoxville, Tennessee 37929
Telephone (866) 252-0878
Email: gklinger@milberg.com

25 Jeff Ostrow*
26 **KOPELOWITZ OSTROW P.A.**
One West Las Olas Blvd, Suite 500
Fort Lauderdale, FL 33301

Tel: (954) 525-4100
Fax: (954) 525-4300
ostrow@kolawyers.com

Counsel for Plaintiff and the Putative Class

**pro hac vice forthcoming*